FIG. 1

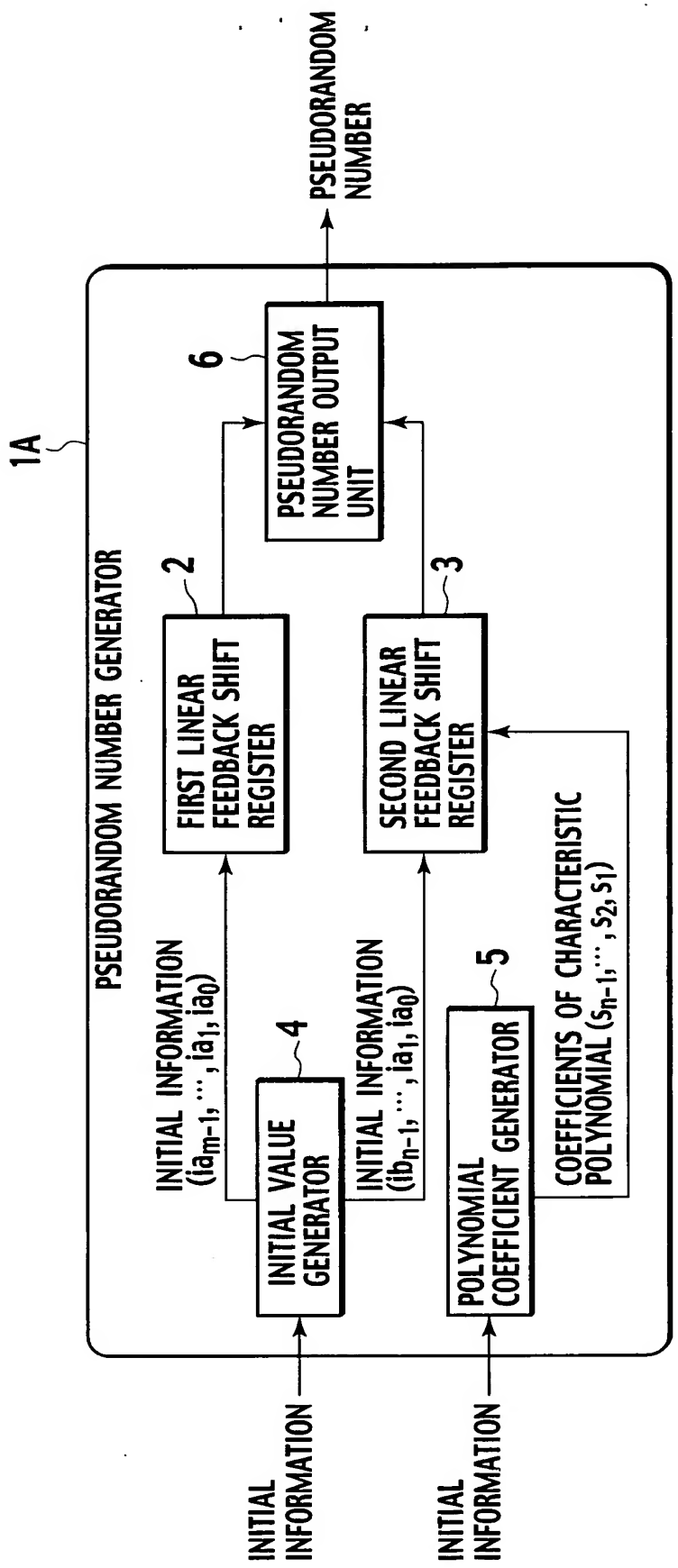

PSEUDORANDOM NUMBER
1A
PSEUDORANDOM NUMBER GENERATOR
6
PSEUDORANDOM NUMBER OUTPUT UNIT
2
FIRST LINEAR FEEDBACK SHIFT REGISTER
3
SECOND LINEAR FEEDBACK SHIFT REGISTER
INITIAL INFORMATION ($ia_{m-1}, \cdots, ia_1, ia_0$)
INITIAL INFORMATION ($ib_{n-1}, \cdots, ia_1, ia_0$)
4
INITIAL VALUE GENERATOR
5
POLYNOMIAL COEFFICIENT GENERATOR
COEFFICIENTS OF CHARACTERISTIC POLYNOMIAL ($s_{n-1}, \cdots, s_2, s_1$)
INITIAL INFORMATION
INITIAL INFORMATION

FIG. 2

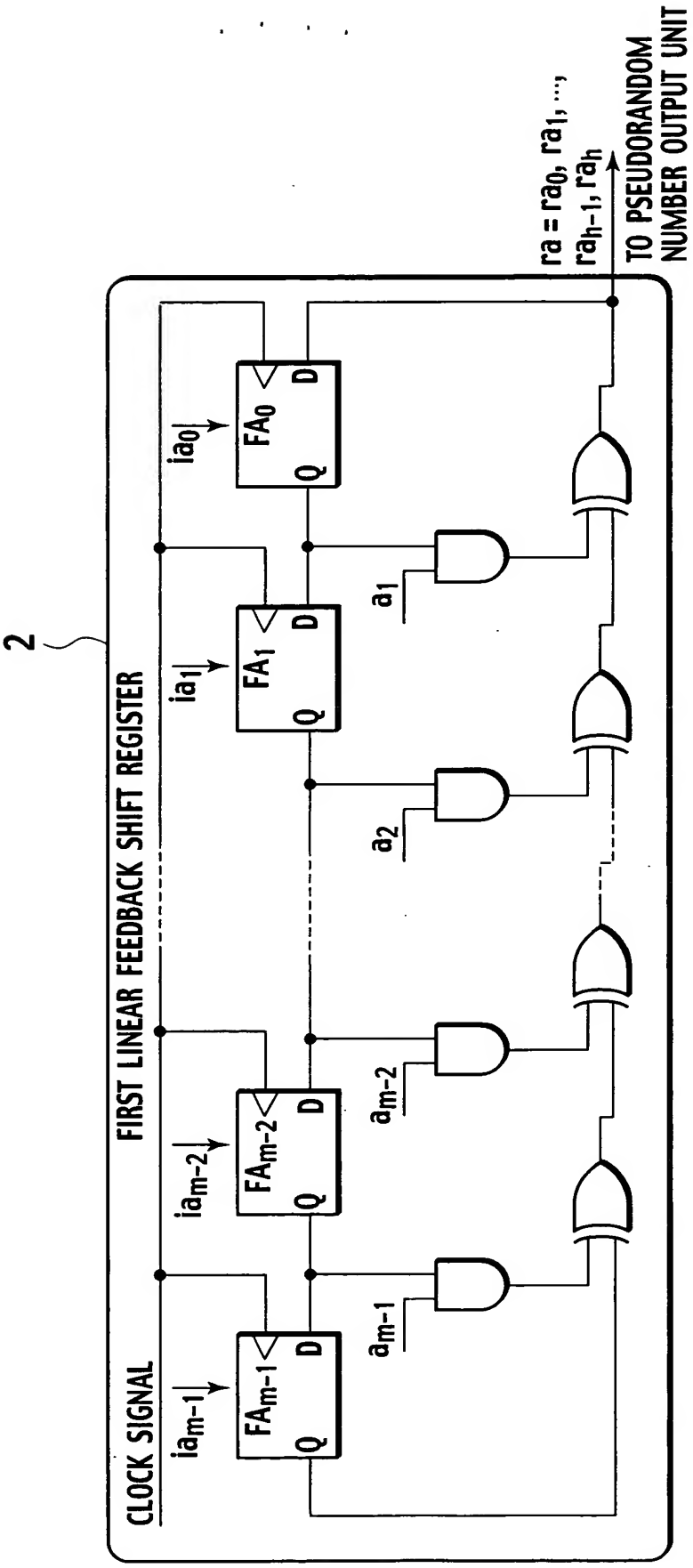

2
FIRST LINEAR FEEDBACK SHIFT REGISTER
CLOCK SIGNAL
ia_{m-1}
FA_{m-1}
ia_{m-2}
FA_{m-2}
ia_1
FA_1
ia_0
FA_0
D
Q
a_{m-1}
a_{m-2}
a_2
a_1
$ra = ra_0, ra_1, \ldots, ra_{h-1}, ra_h$
TO PSEUDORANDOM NUMBER OUTPUT UNIT

FIG. 3

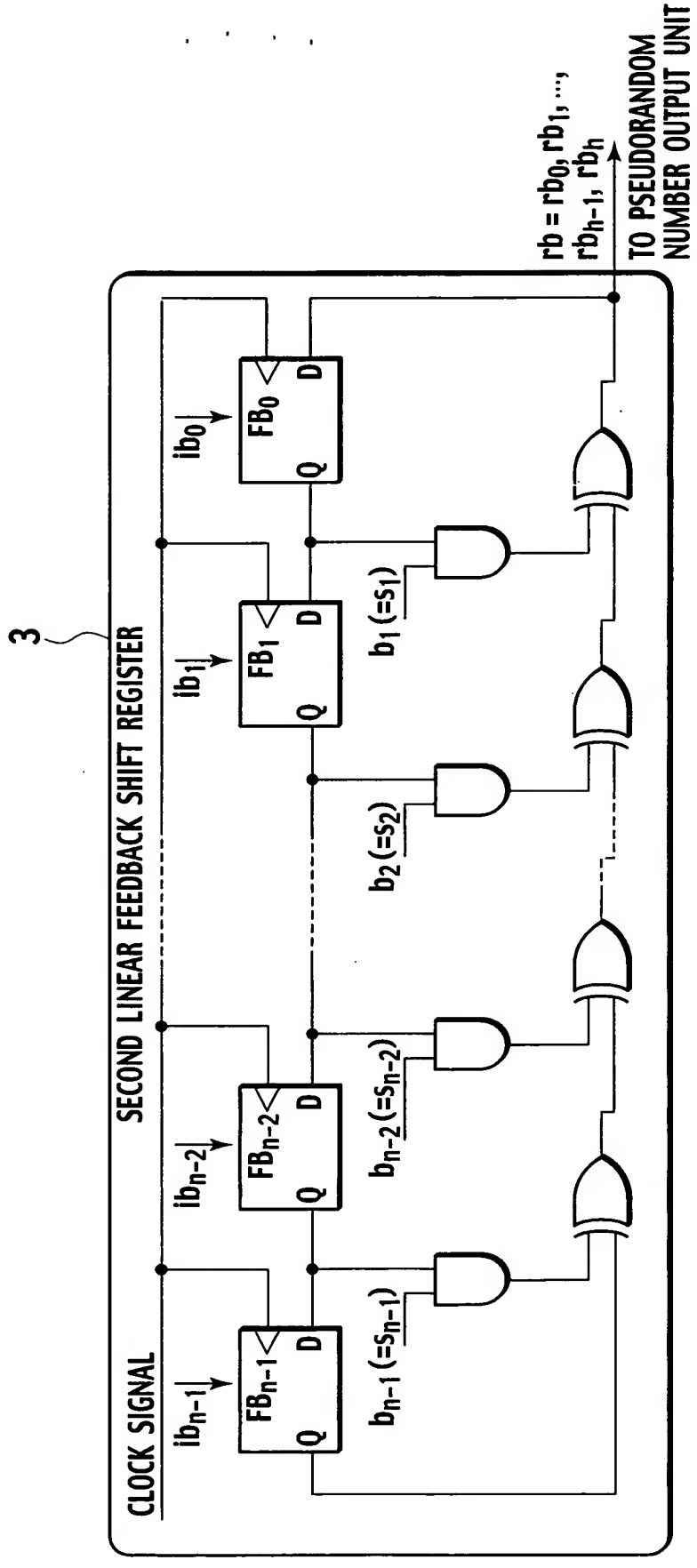

3
SECOND LINEAR FEEDBACK SHIFT REGISTER
CLOCK SIGNAL
ib0
ib1
ibn-2
ibn-1
FB0
FB1
FBn-2
FBn-1
D
Q
b1 (=s1)
b2 (=s2)
bn-2 (=sn-2)
bn-1 (=sn-1)
rb = rb0, rb1, ...,
rbh-1, rbh
TO PSEUDORANDOM
NUMBER OUTPUT UNIT

FIG. 4

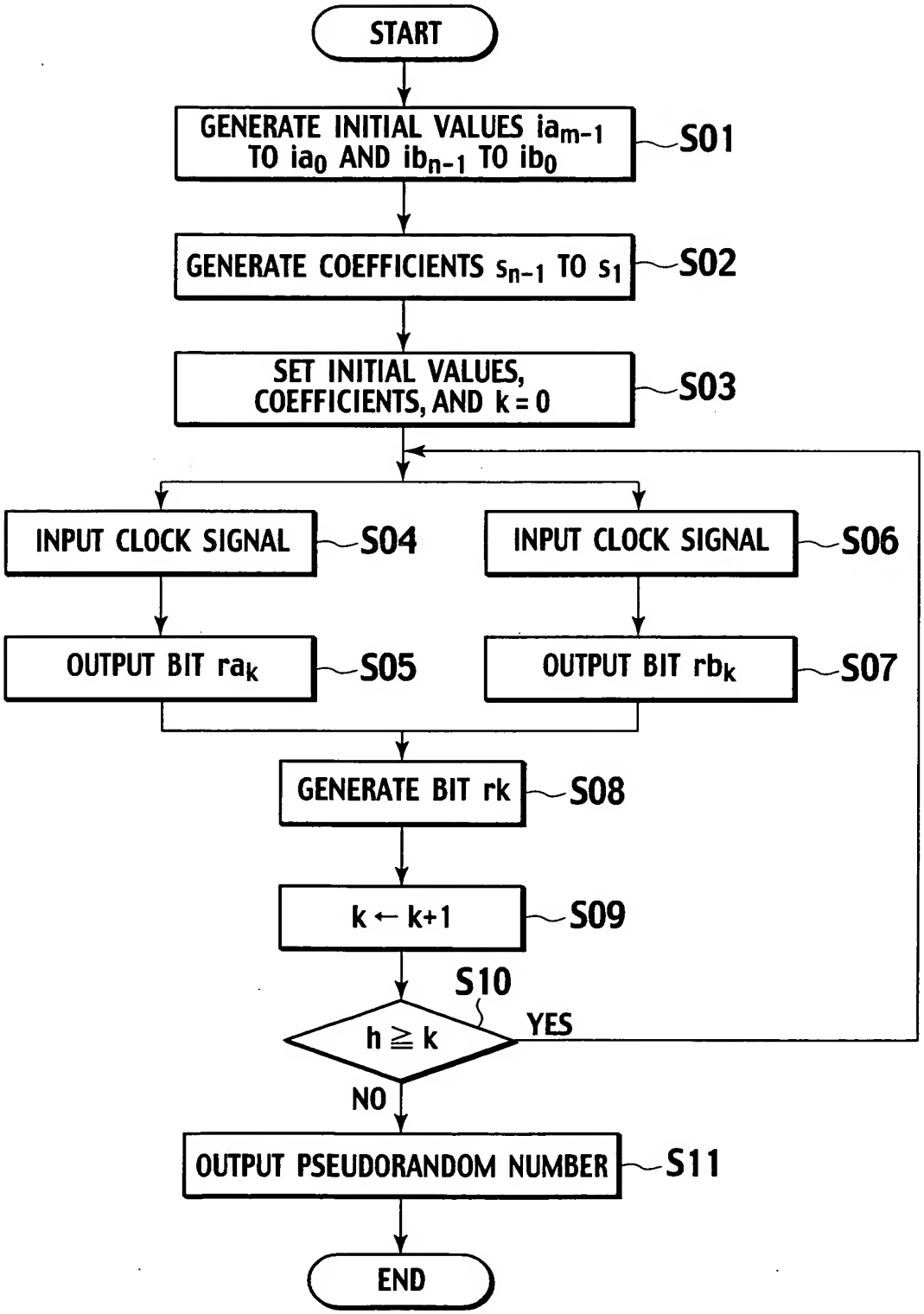

START
GENERATE INITIAL VALUES ia_{m-1} TO ia_0 AND ib_{n-1} TO ib_0
S01
GENERATE COEFFICIENTS s_{n-1} TO s_1
S02
SET INITIAL VALUES, COEFFICIENTS, AND k = 0
S03
INPUT CLOCK SIGNAL
S04
OUTPUT BIT ra_k
S05
INPUT CLOCK SIGNAL
S06
OUTPUT BIT rb_k
S07
GENERATE BIT rk
S08
k ← k+1
S09
S10
h ≧ k
YES
NO
OUTPUT PSEUDORANDOM NUMBER
S11
END

FIG. 5

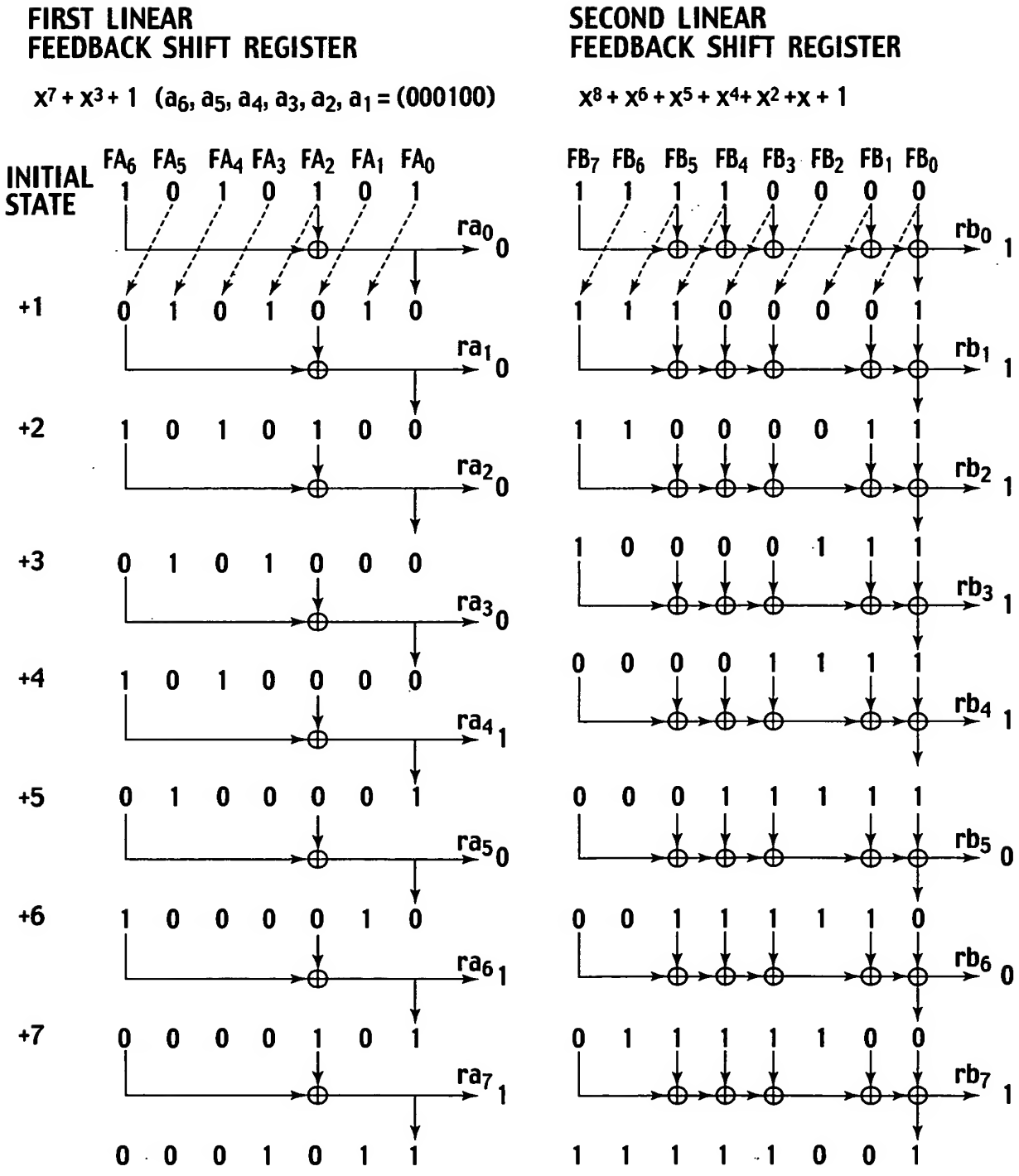

FIRST LINEAR
FEEDBACK SHIFT REGISTER
$x^7 + x^3 + 1$ $(a_6, a_5, a_4, a_3, a_2, a_1 = (000100)$
SECOND LINEAR
FEEDBACK SHIFT REGISTER
$x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$
INITIAL STATE
FA_6 FA_5 FA_4 FA_3 FA_2 FA_1 FA_0
FB_7 FB_6 FB_5 FB_4 FB_3 FB_2 FB_1 FB_0
+1
+2
+3
+4
+5
+6
+7
ra_0 ra_1 ra_2 ra_3 ra_4 ra_5 ra_6 ra_7
rb_0 rb_1 rb_2 rb_3 rb_4 rb_5 rb_6 rb_7

FIG. 6

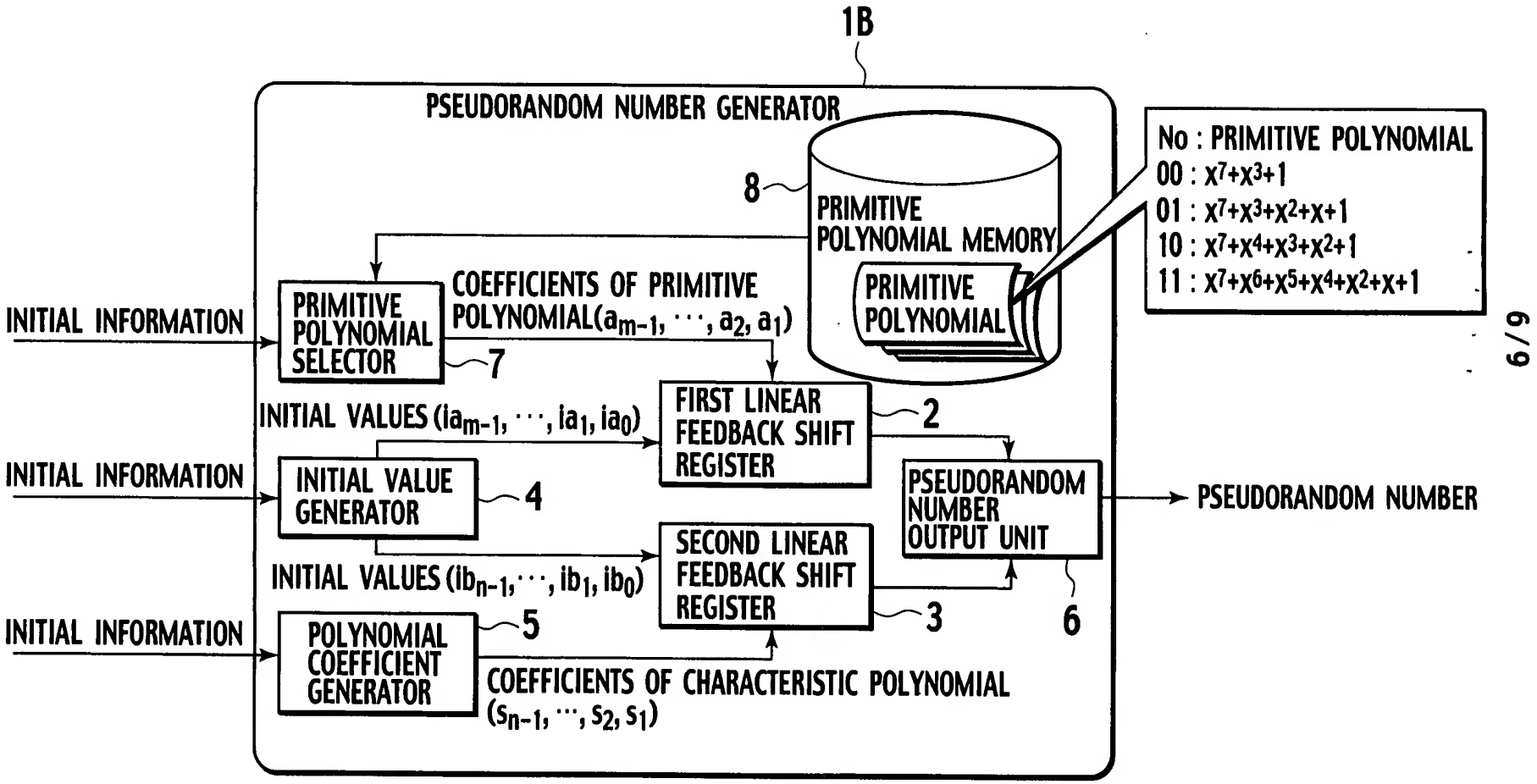

1B
PSEUDORANDOM NUMBER GENERATOR
8
PRIMITIVE POLYNOMIAL MEMORY
PRIMITIVE POLYNOMIAL
No : PRIMITIVE POLYNOMIAL
00 : x7+x3+1
01 : x7+x3+x2+x+1
10 : x7+x4+x3+x2+1
11 : x7+x6+x5+x4+x2+x+1
INITIAL INFORMATION
PRIMITIVE POLYNOMIAL SELECTOR
7
COEFFICIENTS OF PRIMITIVE POLYNOMIAL(am-1, ···, a2, a1)
INITIAL VALUES (iam-1, ···, ia1, ia0)
FIRST LINEAR FEEDBACK SHIFT REGISTER
2
INITIAL INFORMATION
INITIAL VALUE GENERATOR
4
PSEUDORANDOM NUMBER OUTPUT UNIT
PSEUDORANDOM NUMBER
INITIAL VALUES (ibn-1, ···, ib1, ib0)
SECOND LINEAR FEEDBACK SHIFT REGISTER
3
6
INITIAL INFORMATION
POLYNOMIAL COEFFICIENT GENERATOR
5
COEFFICIENTS OF CHARACTERISTIC POLYNOMIAL (sn-1, ···, s2, s1)

FIG. 7

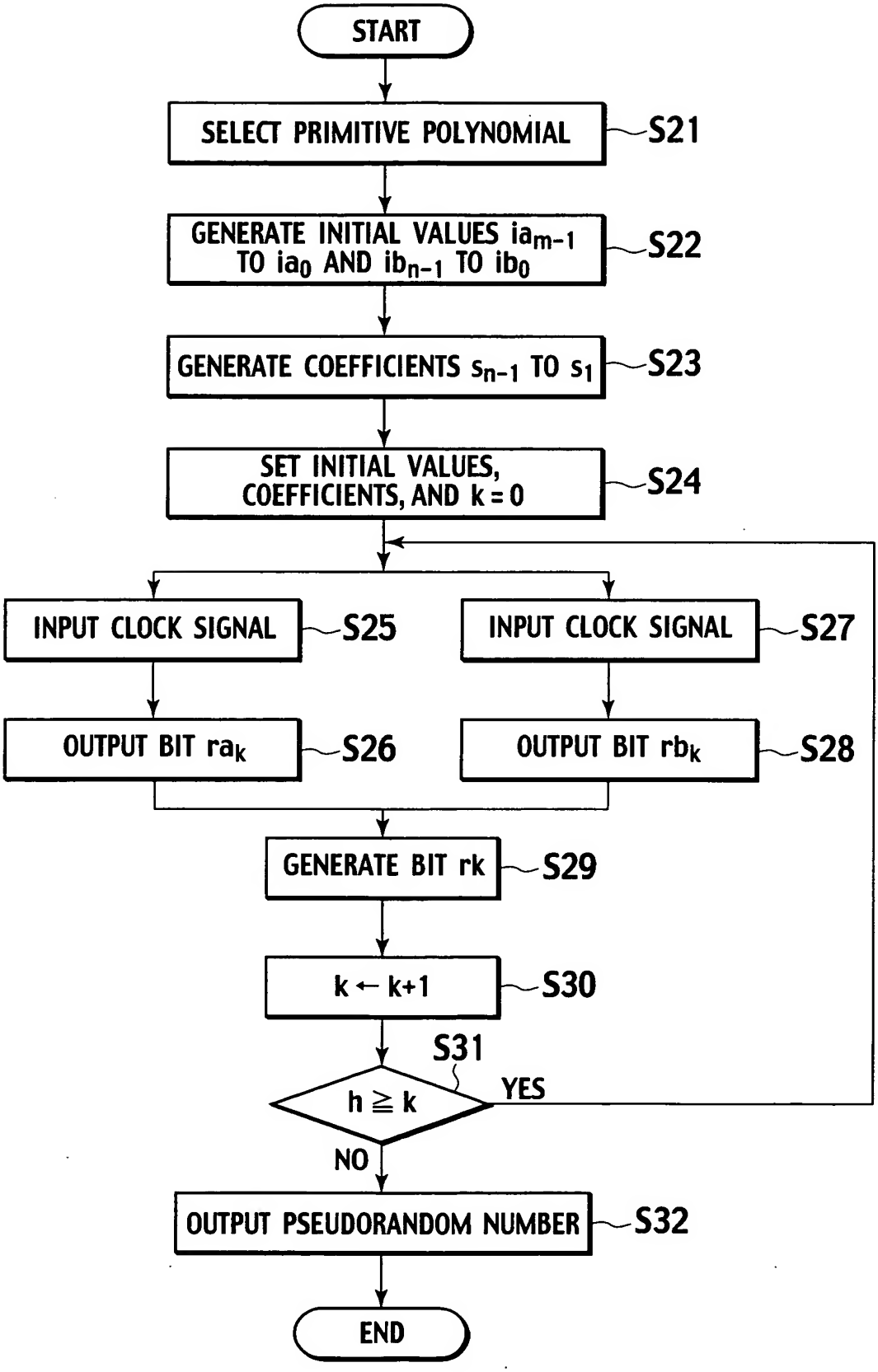

START
SELECT PRIMITIVE POLYNOMIAL
S21
GENERATE INITIAL VALUES ia_{m-1} TO ia_0 AND ib_{n-1} TO ib_0
S22
GENERATE COEFFICIENTS s_{n-1} TO s_1
S23
SET INITIAL VALUES, COEFFICIENTS, AND k = 0
S24
INPUT CLOCK SIGNAL
S25
OUTPUT BIT ra_k
S26
INPUT CLOCK SIGNAL
S27
OUTPUT BIT rb_k
S28
GENERATE BIT rk
S29
k ← k+1
S30
S31
h ≧ k
YES
NO
OUTPUT PSEUDORANDOM NUMBER
S32
END

FIG. 8

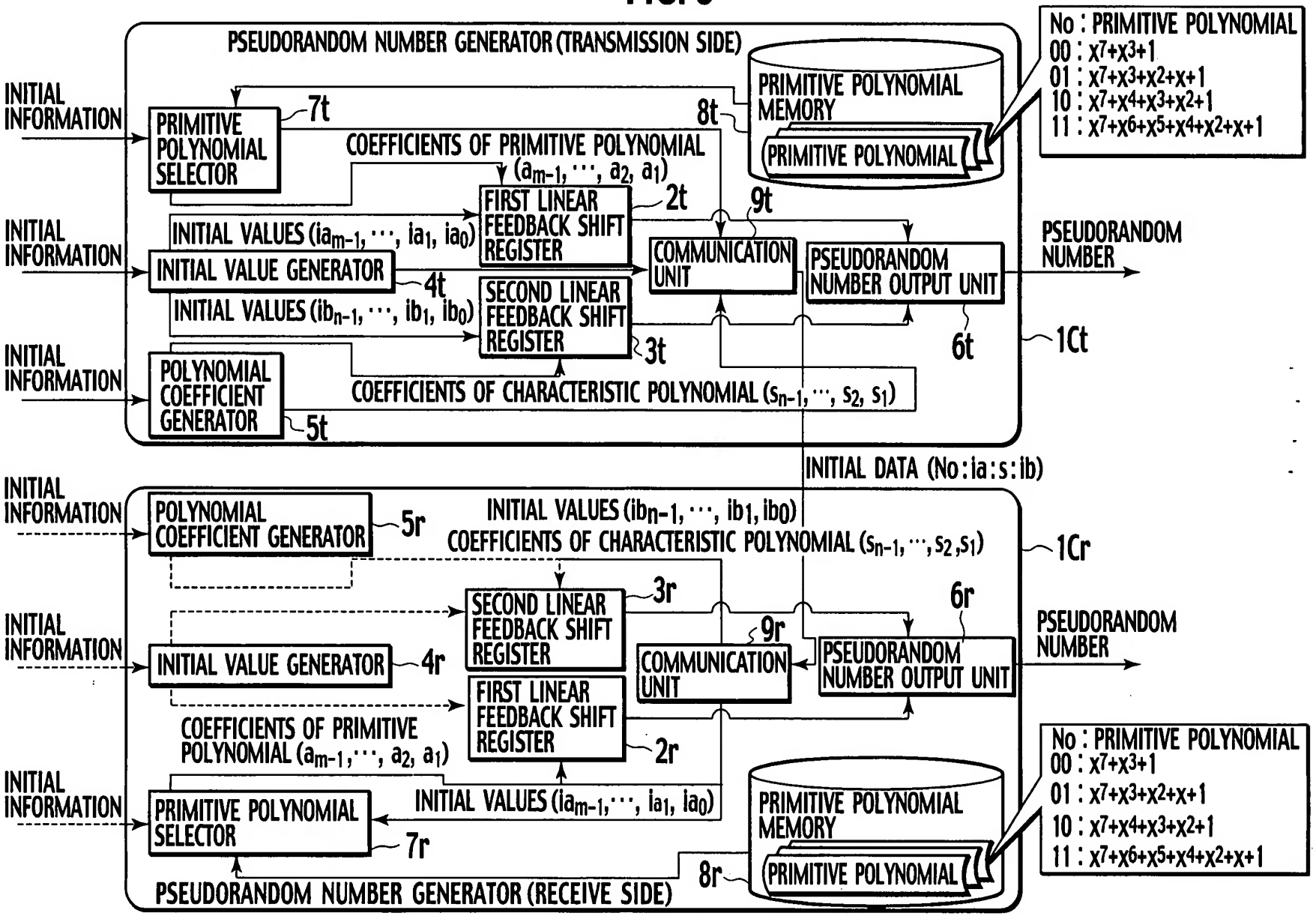
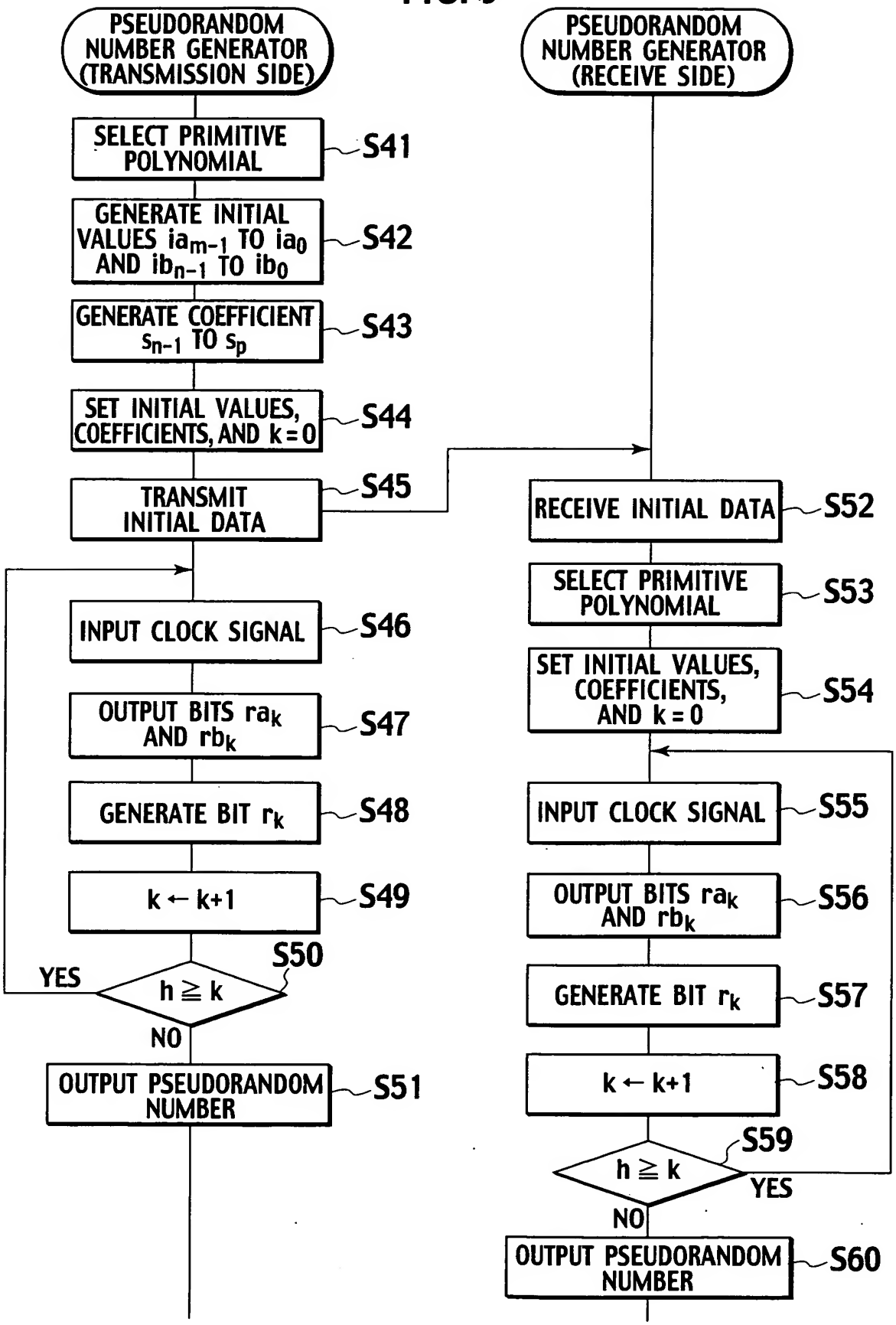

PSEUDORANDOM NUMBER GENERATOR (TRANSMISSION SIDE)
INITIAL INFORMATION
PRIMITIVE POLYNOMIAL SELECTOR
7t
8t
PRIMITIVE POLYNOMIAL MEMORY
PRIMITIVE POLYNOMIAL
COEFFICIENTS OF PRIMITIVE POLYNOMIAL (a_{m-1}, ···, a_2, a_1)
FIRST LINEAR FEEDBACK SHIFT REGISTER
2t
9t
INITIAL VALUES (ia_{m-1}, ···, ia_1, ia_0)
INITIAL VALUE GENERATOR
4t
COMMUNICATION UNIT
PSEUDORANDOM NUMBER OUTPUT UNIT
PSEUDORANDOM NUMBER
SECOND LINEAR FEEDBACK SHIFT REGISTER
INITIAL VALUES (ib_{n-1}, ···, ib_1, ib_0)
3t
6t
1Ct
POLYNOMIAL COEFFICIENT GENERATOR
5t
COEFFICIENTS OF CHARACTERISTIC POLYNOMIAL (s_{n-1}, ···, s_2, s_1)
No : PRIMITIVE POLYNOMIAL
00 : x^7+x^3+1
01 : $x^7+x^3+x^2+x+1$
10 : $x^7+x^4+x^3+x^2+1$
11 : $x^7+x^6+x^5+x^4+x^2+x+1$
INITIAL DATA (No:ia:s:ib)
POLYNOMIAL COEFFICIENT GENERATOR
5r
INITIAL VALUES (ib_{n-1}, ···, ib_1, ib_0)
COEFFICIENTS OF CHARACTERISTIC POLYNOMIAL (s_{n-1}, ···, s_2, s_1)
1Cr
SECOND LINEAR FEEDBACK SHIFT REGISTER
3r
6r
9r
INITIAL VALUE GENERATOR
4r
COMMUNICATION UNIT
PSEUDORANDOM NUMBER OUTPUT UNIT
PSEUDORANDOM NUMBER
FIRST LINEAR FEEDBACK SHIFT REGISTER
2r
COEFFICIENTS OF PRIMITIVE POLYNOMIAL (a_{m-1}, ···, a_2, a_1)
PRIMITIVE POLYNOMIAL SELECTOR
7r
INITIAL VALUES (ia_{m-1}, ···, ia_1, ia_0)
PRIMITIVE POLYNOMIAL MEMORY
PRIMITIVE POLYNOMIAL
8r
PSEUDORANDOM NUMBER GENERATOR (RECEIVE SIDE)
No : PRIMITIVE POLYNOMIAL
00 : x^7+x^3+1
01 : $x^7+x^3+x^2+x+1$
10 : $x^7+x^4+x^3+x^2+1$
11 : $x^7+x^6+x^5+x^4+x^2+x+1$

FIG. 9


PSEUDORANDOM NUMBER GENERATOR (TRANSMISSION SIDE)
SELECT PRIMITIVE POLYNOMIAL
S41
GENERATE INITIAL VALUES ia_{m-1} TO ia_0 AND ib_{n-1} TO ib_0
S42
GENERATE COEFFICIENT s_{n-1} TO s_p
S43
SET INITIAL VALUES, COEFFICIENTS, AND k = 0
S44
TRANSMIT INITIAL DATA
S45
INPUT CLOCK SIGNAL
S46
OUTPUT BITS ra_k AND rb_k
S47
GENERATE BIT r_k
S48
k ← k+1
S49
S50
h ≧ k
YES
NO
OUTPUT PSEUDORANDOM NUMBER
S51
PSEUDORANDOM NUMBER GENERATOR (RECEIVE SIDE)
RECEIVE INITIAL DATA
S52
SELECT PRIMITIVE POLYNOMIAL
S53
SET INITIAL VALUES, COEFFICIENTS, AND k = 0
S54
INPUT CLOCK SIGNAL
S55
OUTPUT BITS ra_k AND rb_k
S56
GENERATE BIT r_k
S57
k ← k+1
S58
S59
h ≧ k
YES
NO
OUTPUT PSEUDORANDOM NUMBER
S60